09/963,455

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日 Date of Application:	２０００年　９月２９日
出願番号 Application Number:	特願２０００－２９７９３７
出願人 Applicant(s):	株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　９月１８日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０８５７７１

【書類名】　特許願
【整理番号】　K00015381
【あて先】　特許庁長官殿
【国際特許分類】　G06F 15/00
【発明者】
【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所　公共システム事業部内
【氏名】　斎藤　司
【発明者】
【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所　公共システム事業部内
【氏名】　三浦　信治
【発明者】
【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所　公共システム事業部内
【氏名】　村上　剛司
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社日立製作所
【代理人】
【識別番号】　100083552
【弁理士】
【氏名又は名称】　秋田　収喜
【電話番号】　03-3893-6221
【手数料の表示】
【予納台帳番号】　014579
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　アクセス制御方法及びその実施装置並びにその処理プログラムを記録した記録媒体

【特許請求の範囲】

【請求項１】　利用者から受付けたアクセス内容の実行を制御するアクセス制御方法において、

利用者から要求されたアクセスの内容を示すアクセス内容を受付けるステップと、前記受付けたアクセス内容の実行を当該利用者の利用者属性と共に要求するステップと、前記要求されたアクセス内容の処理をそのアクセス内容と共に送られた利用者属性に対応する範囲内で実行するステップとを有することを特徴とするアクセス制御方法。

【請求項２】　前記利用者属性の開示内容を利用者属性開示ポリシーに従って制限することを特徴とする請求項１に記載されたアクセス制御方法。

【請求項３】　前記利用者属性の開示先を利用者属性開示ポリシーに従って制限することを特徴とする請求項１または請求項２のいずれかに記載されたアクセス制御方法。

【請求項４】　利用者から受付けたアクセス内容の実行を制御するアクセス制御システムにおいて、

利用者から要求されたアクセスの内容を示すアクセス内容を受付けるアクセス依頼処理部と、前記受付けたアクセス内容の実行を当該利用者の利用者属性と共に要求するアクセス要求処理部と、前記要求されたアクセス内容の処理をそのアクセス内容と共に送られた利用者属性に対応する範囲内で実行するアクセス実行処理部とを備えることを特徴とするアクセス制御システム。

【請求項５】　利用者から受付けたアクセス内容の実行を制御するアクセス制御システムとしてコンピュータを機能させる為のプログラムを記録したコンピュータ読み取り可能な記録媒体において、

利用者から要求されたアクセスの内容を示すアクセス内容を受付けるアクセス依頼処理部と、前記受付けたアクセス内容の実行を当該利用者の利用者属性と共に要求するアクセス要求処理部と、前記要求されたアクセス内容の処理をそのア

クセス内容と共に送られた利用者属性に対応する範囲内で実行するアクセス実行処理部としてコンピュータを機能させる為のプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は利用者から受付けたアクセス内容の実行を制御するアクセス制御システムに関し、特に利用者から受付けた情報要求内容の検索をその利用者の利用者属性に応じて制御するアクセス制御システムに適用して有効な技術に関するものである。

【０００２】

【従来の技術】

従来、インターネット上のサイトでは各種情報の発信が行われており、それらのサイトへアクセスすることにより、誰でもが多くの情報を参照することができる。この様なインターネット上で情報を発信しようとする場合には、インターネット上でサイトを開設し、発信しようとする情報が書き込まれたＨＴＭＬ(Hyper Text Markup Language)等のファイルを作成しておき、誰でもがその情報を読み出せる様にそのファイルへのアクセス権限を設定しておけば良い。

【０００３】

この様にして不特定多数の利用者に対して発信されている情報を参照しようとする場合、利用者は、インターネット上の検索サイトを利用して特定のキーワードを含むサイトを検索したり、他のサイトに設けられているリンクを辿ったりして目的のサイトに遷移し、そのサイトから発信されている情報を参照することができる。例えば、ある利用者がインフルエンザに関する情報を収集しようとする際には、検索サイトでキーワード「インフルエンザ」を入力して検索を行うことにより、単語「インフルエンザ」を含む情報を開示しているサイトを検索することができる。

【０００４】

また、情報を発信しているサイトへのアクセスに制限を設け、特定の利用者だ

けにそのサイトの情報を開示する場合もある。この様なアクセス制限では、予め特定の利用者に対してユーザ登録を行ってユーザＩＤとパスワードを発行しておき、そのユーザＩＤ及びパスワードを入力した特定の利用者のみにその情報へのアクセスを許可する等の方法が用いられている。

【０００５】

なお特定の権限を持つ人だけに文書やプログラムなどの利用を許可したり、インターネット上で提供するサービスにおいて、会員の持つ資格によって利用できるサービスや閲覧できる情報の内容を切り換えることが可能なアクセス制御方法及びシステム及びアクセス制御プログラムを格納した記憶媒体については特開平１０－３２０２８８号公報に記載されている。その概要は、個々の利用者を区別するための利用者識別情報と該利用者の分類情報を保持し、あるオブジェクトがどの範囲の利用者から利用可能かを表す利用範囲情報とオブジェクト本体を一体的に格納し、利用者がオブジェクトを要求すると、利用者の要求するオブジェクトが該利用者から利用可能かどうかを、利用者識別情報、利用者の分類情報及び、利用範囲情報を参照して判定し個々のオブジェクト毎に利用範囲情報に対応する利用者のみにオブジェクトの利用を許可し、オブジェクトを提供するものである。

【０００６】

【発明が解決しようとする課題】

前記従来の技術において、任意の利用者からのアクセスを許可しているインターネット上のサイトでは、アクセスしているのがどういった利用者であるかに関わらず同様の処理が行われる為、利用者が望む結果が得られない場合が生じるという問題がある。

【０００７】

例えば、ある利用者がインフルエンザに関する情報を収集しようとする際には、一般の人がインフルエンザとはどういうものであるかを知りたい場合や、医師が最新のウィルス種別及び対応ワクチンについて調査したい場合等、その利用者によって必要とする情報の内容が異なってくるが、検索サイトで「インフルエンザ」を検索した場合には、利用者がどういった人間であるかに関わらず、キーワ

ード「インフルエンザ」を含む全てのサイトが検索される為、利用者は、それらの多くのサイトの情報の中から自分の望む情報がどれであるかを探さなければならない。

【０００８】

前記従来の様に利用者が望む結果が得られない場合には、利用者毎に木目細かなアクセス制御を行うことが望まれるが、前記の様なインターネット上のアクセスでは、不特定の利用者が不特定のサイトへアクセスすることが多い為、ユーザＩＤ及びパスワード等によるユーザ管理ではそのユーザ管理に必要な負担が増大するという問題がある。

【０００９】

すなわち前記従来の技術において、ユーザＩＤ及びパスワード等によって利用者毎に異なるアクセス制御を行おうとした場合、利用者は目的とする情報が得られそうな全てのサイトで予めユーザＩＤ及びパスワードを取得して管理し、またサイト運営者はアクセスを希望する全ての利用者毎に異なるアクセス権限を設定して管理する必要がある為、不特定多数の利用者が不特定多数のサイトへアクセスすることを想定した場合では、管理対象のユーザＩＤ及びパスワードの数が増大し、それらを管理することが実質的に不可能になるという問題がある。

【００１０】

本発明の目的は上記問題を解決し、要求されたアクセス内容の実行側での利用者管理等の負担を増やすことなく利用者毎に木目細かなアクセス制御を行うことが可能な技術を提供することにある。

【００１１】

【課題を解決するための手段】

本発明は、利用者から受付けたアクセス内容の実行を制御するアクセス制御システムにおいて、利用者が要求したアクセス内容の実行を当該利用者の利用者属性に応じて制御するものである。

【００１２】

本発明のアクセス制御システムでは、まず利用者の各種属性を示す利用者属性をプロバイダ側処理装置に設定しておき、利用者から受付けたアクセス内容の実

行を行うアクセス処理装置に当該利用者の利用者属性に応じたアクセス制御を行う為の情報を設定しておく。

【００１３】

利用者側処理装置では、利用者から要求された情報検索等のアクセスの内容を示すアクセス内容を受付けて、当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーと共にプロバイダ側処理装置に送る。

【００１４】

プロバイダ側処理装置では、前記受付けたアクセス内容の処理を実行するアクセス処理装置を利用者属性開示ポリシーに従って決定し、前記利用者属性の開示先の制限を行う。またプロバイダ側処理装置では、前記決定したアクセス処理装置に対して開示する利用者属性の内容を利用者属性開示ポリシーに従って決定し、前記利用者属性の開示内容の制限を行う。そして前記受付けたアクセス内容及び前記制限した開示内容の利用者属性を前記決定したアクセス処理装置に送り、そのアクセス内容の実行を要求する。

【００１５】

アクセス処理装置では、アクセス内容と共に送られた利用者属性に応じてアクセス制御レベルを設定し、前記要求されたアクセス内容の処理をそのアクセス制御レベルに対応した範囲内で実行する。

【００１６】

以上の様に本発明のアクセス制御システムによれば、利用者から要求されたアクセス内容の実行を当該利用者の利用者属性に応じて制御するので、要求されたアクセス内容の実行側での利用者管理等の負担を増やすことなく利用者毎に木目細かなアクセス制御を行うことが可能である。

【００１７】

【発明の実施の形態】

以下に利用者から受付けたアクセス内容の実行をその利用者の属性情報に応じて制御する一実施形態のアクセス制御システムについて説明する。

【００１８】

図１は本実施形態のアクセス制御システムの概略構成を示す図である。図１に

示す様に本実施形態のアクセス制御システムは、プロバイダ側処理装置１００と、利用者側処理装置１０１と、アクセス処理装置１０２とを有している。

【００１９】

プロバイダ側処理装置１００は、利用者から要求されたアクセスの内容を示すアクセス内容と当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーを利用者側処理装置１０１から受付け、当該利用者属性開示ポリシーに従って決定したアクセス処理装置１０２に当該アクセス内容の処理を要求するプロバイダ側の情報処理装置である。

【００２０】

利用者側処理装置１０１は、アクセス内容及び利用者属性開示ポリシーを利用者から受付けて当該アクセス内容の処理をプロバイダ側処理装置１００に依頼する利用者側の情報処理装置である。アクセス処理装置１０２は、プロバイダ側処理装置１００から要求されたアクセス内容の処理をそのアクセス内容と共に送られた利用者属性に対応する範囲内で実行する情報処理装置である。

【００２１】

図２は本実施形態のプロバイダ側処理装置１００の概略構成を示す図である。図２に示す様に本実施形態のプロバイダ側処理装置１００は、ＣＰＵ２０１と、メモリ２０２と、磁気ディスク装置２０３と、入力装置２０４と、出力装置２０５と、ＣＤ－ＲＯＭ装置２０６と、利用者属性ＤＢ２０７とを有している。

【００２２】

ＣＰＵ２０１は、プロバイダ側処理装置１００全体の動作を制御する装置である。メモリ２０２は、プロバイダ側処理装置１００全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【００２３】

磁気ディスク装置２０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置２０４は、利用者から受付けたアクセス内容の処理をアクセス処理装置１０２に要求する為の各種入力を行う装置である。

【００２４】

出力装置２０５は、利用者から受付けたアクセス内容の処理要求に伴う各種出

力を行う装置である。ＣＤ－ＲＯＭ装置２０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。利用者属性ＤＢ２０７は、利用者の氏名、性別、年齢、職業、勤務先・役職等の各種属性を示す情報を格納するデータベースである。

【００２５】

またプロバイダ側処理装置１００は、利用者属性設定処理部２１０と、開示ポリシー処理部２１１と、アクセス要求処理部２１２とを有している。

【００２６】

利用者属性設定処理部２１０は、利用者の各種属性を示す利用者属性を利用者側処理装置１０１から受信してプロバイダ側処理装置１００内の利用者属性ＤＢ２０７に設定する処理部である。開示ポリシー処理部２１１は、利用者から要求されたアクセスの内容を示すアクセス内容と当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーとを利用者側処理装置１０１から受付け、当該アクセス内容の処理を実行するアクセス処理装置１０２とそのアクセス処理装置１０２に開示する利用者属性の内容とを前記利用者属性開示ポリシーに従って決定する処理部である。アクセス要求処理部２１２は、利用者側処理装置１０１から送信されたアクセス内容の処理を前記利用者属性の開示内容と共に前記決定したアクセス処理装置１０２に要求する処理部である。

【００２７】

プロバイダ側処理装置１００を利用者属性設定処理部２１０、開示ポリシー処理部２１１及びアクセス要求処理部２１２として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００２８】

図３は本実施形態の利用者側処理装置１０１の概略構成を示す図である。図３に示す様に本実施形態の利用者側処理装置１０１は、ＣＰＵ３０１と、メモリ３０２と、磁気ディスク装置３０３と、入力装置３０４と、出力装置３０５と、ＣＤ－ＲＯＭ装置３０６とを有している。

【００２９】

ＣＰＵ３０１は、利用者側処理装置１０１全体の動作を制御する装置である。メモリ３０２は、利用者側処理装置１０１全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【００３０】

磁気ディスク装置３０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置３０４は、利用者から入力されたアクセス内容の処理をプロバイダ側処理装置１００に依頼する為の各種入力を行う装置である。

【００３１】

出力装置３０５は、利用者から入力されたアクセス内容の処理依頼に伴う各種出力を行う装置である。ＣＤ－ＲＯＭ装置３０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。

【００３２】

また利用者側処理装置１０１は、利用者属性設定依頼処理部３１０と、アクセス依頼処理部３１１とを有している。

【００３３】

利用者属性設定依頼処理部３１０は、利用者側処理装置１０１を利用する利用者の各種属性を表す利用者属性の設定をプロバイダ側処理装置１００に依頼する処理部である。アクセス依頼処理部３１１は、利用者から要求されたアクセスの内容を示すアクセス内容と当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーとを受付けて当該アクセス内容の処理をプロバイダ側処理装置１００に依頼する処理部である。

【００３４】

利用者側処理装置１０１を利用者属性設定依頼処理部３１０及びアクセス依頼処理部３１１として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００３５】

図４は本実施形態のアクセス処理装置１０２の概略構成を示す図である。図４に示す様に本実施形態のアクセス処理装置１０２は、ＣＰＵ４０１と、メモリ４０２と、磁気ディスク装置４０３と、入力装置４０４と、出力装置４０５と、ＣＤ－ＲＯＭ装置４０６と、アクセス制御情報ＤＢ４０７とを有している。

【００３６】

ＣＰＵ４０１は、アクセス処理装置１０２全体の動作を制御する装置である。メモリ４０２は、アクセス処理装置１０２全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【００３７】

磁気ディスク装置４０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置４０４は、プロバイダ側処理装置１００から要求されたアクセス内容の処理を実行する為の各種入力を行う装置である。

【００３８】

出力装置４０５は、プロバイダ側処理装置１００から要求されたアクセス内容の処理実行に伴う各種出力を行う装置である。ＣＤ－ＲＯＭ装置４０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。アクセス制御情報ＤＢ４０７は、アクセス処理装置１０２でサイトを公開しているサイト公開者の各種属性や、利用者属性に応じたアクセス制御内容を示す情報を格納するデータベースである。

【００３９】

またアクセス処理装置１０２は、アクセス制御情報設定処理部４１０と、アクセス実行処理部４１１とを有している。

【００４０】

アクセス制御情報設定処理部４１０は、アクセス処理装置１０２でサイトを公開しているサイト公開者の各種属性や、利用者属性に応じたアクセス制御内容を示す情報をアクセス制御情報ＤＢ４０７に設定する処理部である。アクセス実行処理部４１１は、プロバイダ側処理装置１００から要求されたアクセス内容の処理をそのアクセス内容と共に送られた利用者属性に対応する範囲内で実行する処理部である。

【００４１】

アクセス処理装置１０２をアクセス制御情報設定処理部４１０及びアクセス実行処理部４１１として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００４２】

本実施形態の利用者側処理装置１０１の利用者属性設定依頼処理部３１０は、利用者側処理装置１０１を利用する利用者の氏名、性別、年齢、職業、勤務先・役職等の利用者属性の設定をプロバイダ側処理装置１００に依頼する処理を行い、プロバイダ側処理装置１００の利用者属性設定処理部２１０は、前記利用者属性を利用者側処理装置１０１から受信してプロバイダ側処理装置１００内の利用者属性ＤＢ２０７に設定する処理を行う。

【００４３】

図５は本実施形態の利用者属性ＤＢ２０７の一例を示す図である。図５に示す様に本実施形態の利用者属性ＤＢ２０７には、利用者側処理装置１０１を利用する利用者の利用者属性として、氏名、性別、年齢、職業、勤務先・役職等の情報が格納されている。

【００４４】

本実施形態のアクセス処理装置１０２のアクセス制御情報設定処理部４１０は、アクセス処理装置１０２でサイトを公開しているサイト公開者の各種属性や、利用者属性に応じたアクセス制御内容を示す情報をアクセス制御情報ＤＢ４０７に設定する処理を行う。

【００４５】

図６は本実施形態のアクセス制御情報ＤＢ４０７の一例を示す図である。図６に示す様に本実施形態のアクセス制御情報ＤＢ４０７には、アクセス処理装置１０２でサイトを公開しているサイト公開者の属性として、サイト公開者名、サイト情報が格納され、プロバイダ側処理装置１００からアクセス内容の処理を要求された場合にその利用者属性に応じたアクセス範囲を示すレベルを設定する為の

情報提供ポリシー、前記設定したレベルに応じた制御内容を示すアクセス制御情報が格納されている。ここで、サイト公開者名やサイト情報等の情報に第３者機関の認証情報を付加してその改竄を防止しているものとする。

【００４６】

この図６では、インフルエンザに関する情報検索を行う場合の情報提供ポリシー及びアクセス制御情報を示しており、他のアクセス内容について情報提供ポリシーを設定する場合にはその職業や役職の違いに応じて異なるアクセス制御レベルを設定し、またそれらのアクセス制御レベルに対応するアクセス制御情報にはアクセス制御レベルが高くなるに従ってより高度な情報へのアクセスが可能な制御情報が設定されるものとする。

【００４７】

以下に本実施形態のアクセス制御システムにおいて、利用者側処理装置１０１からアクセス内容の処理をプロバイダ側処理装置１００に依頼し、当該アクセス内容の処理を実行するアクセス処理装置１０２とそのアクセス処理装置１０２に開示する利用者属性の内容とを利用者属性開示ポリシーに従って決定する処理をプロバイダ側処理装置１００で行い、前記決定された開示内容の利用者属性に対応する範囲内で当該アクセス内容の処理をアクセス処理装置１０２で実行する処理について説明する。

【００４８】

図７は本実施形態のアクセス依頼処理の処理手順を示すフローチャートである。図７に示す様に利用者側処理装置１０１のアクセス依頼処理部３１１は、利用者から要求されたアクセスの内容を示すアクセス内容と当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーとを受付けて当該アクセス内容の処理をプロバイダ側処理装置１００に依頼する処理を行う。

【００４９】

本実施形態のアクセス制御システムにおいて、利用者がインターネット等のネットワークで接続された各アクセス処理装置に対して情報検索等のアクセス内容の処理を要求する場合には、プロバイダ側処理装置１００にログインしてそのネットワークに接続した後、そのアクセス内容と、その処理を実行する際に当該利

用者の利用者属性をどれだけアクセス処理装置１０２へ開示するかを示す利用者属性開示ポリシーを利用者側処理装置１０１に入力する。

【００５０】

ステップ７０１で利用者側処理装置１０１のアクセス依頼処理部３１１は、プロバイダ側処理装置１００にログインする為のユーザＩＤ及びパスワードの入力を利用者から受付けてそれらの情報をプロバイダ側処理装置１００へ送り、プロバイダ側処理装置１００にログインする。

【００５１】

ステップ７０２では、利用者が要求するアクセス内容の入力が行われたかどうかを調べ、アクセス内容の入力が行われた場合にはステップ７０３へ進む。ステップ７０３では、前記入力されたアクセス内容を受付けてアクセス内容情報としてメモリ３０２に格納する。

【００５２】

ステップ７０４では、当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーの入力が行われたかどうかを調べ、利用者属性開示ポリシーの入力が行われた場合にはステップ７０５へ進む。ステップ７０５では、前記入力された利用者属性開示ポリシーを受付けて利用者属性開示ポリシー情報としてメモリ３０２に格納する。

【００５３】

ステップ７０６では、前記格納したアクセス内容情報及び利用者属性開示ポリシー情報をネットワーク経由でプロバイダ側処理装置１００に送り、当該アクセス内容の処理をプロバイダ側処理装置１００へ依頼する。

【００５４】

ステップ７０７では、前記依頼したアクセス内容の処理結果をプロバイダ側処理装置１００から受信しているかどうかを調べ、アクセス内容の処理結果を受信している場合にはステップ７０８へ進む。ステップ７０８では、前記受信した処理結果を出力装置３０５へ表示する。

【００５５】

図８は本実施形態のアクセス要求処理の処理手順を示すフローチャートである

。図８に示す様にプロバイダ側処理装置１００の開示ポリシー処理部２１１は、利用者から要求されたアクセスの内容を示すアクセス内容と当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーとを利用者側処理装置１０１から受付け、当該アクセス内容の処理を実行するアクセス処理装置１０２とそのアクセス処理装置１０２に開示する利用者属性の内容とを前記利用者属性開示ポリシーに従って決定する処理を行い、そしてアクセス要求処理部２１２は、利用者側処理装置１０１から送信されたアクセス内容の処理を前記利用者属性の開示内容と共に前記決定したアクセス処理装置１０２に要求する処理を行う。

【００５６】

ステップ８０１でプロバイダ側処理装置１００の開示ポリシー処理部２１１は、アクセス内容の処理依頼を利用者側処理装置１０１から受信しているかどうかを調べ、アクセス内容の処理依頼を受信している場合にはステップ８０２へ進む。

【００５７】

ステップ８０２では、前記受信したアクセス内容の処理が可能なアクセス処理装置１０２からサイト情報を受信する。ステップ８０３では、利用者側処理装置１０１から受信した利用者属性開示ポリシーとアクセス処理装置１０２から受信したサイト情報とを比較して、そのアクセス処理装置１０２が利用者属性開示ポリシーで示された条件を満たしているかどうかを調べる認証処理を行い、利用者属性開示ポリシーの条件を満たしている場合にはステップ８０４へ進む。ステップ８０４では、利用者属性開示ポリシーの条件を満たしているアクセス処理装置１０２を当該アクセス内容の処理を実行する処理装置として設定する。

【００５８】

ステップ８０５では、前記受信したアクセス内容の処理が可能な全てのアクセス処理装置１０２からサイト情報を受信したかどうかを調べ、またサイト情報を受信していないアクセス処理装置１０２がある場合にはステップ８０２へ戻り、全てのアクセス処理装置１０２からサイト情報を受信し終えた場合にはステップ８０６へ進む。

【００５９】

なお本実施形態では前記の様に各アクセス処理装置１０２からサイト情報を受信して利用者属性開示ポリシーの条件を満たしているかどうかを判定しているが、予め各アクセス処理装置１０２からサイト情報を受信してプロバイダ側処理装置１００に格納しておき、利用者側処理装置１０１から受信した利用者属性開示ポリシーとプロバイダ側処理装置１００に格納されたサイト情報とを比較して、利用者属性開示ポリシーの条件を満たしているかどうかを判定しても良い。

【００６０】

ステップ８０６では、利用者側処理装置１０１から受信した利用者属性開示ポリシーに従って当該利用者のユーザＩＤに対応する利用者属性を利用者属性ＤＢ２０７から読み出して、アクセス処理装置１０２へ開示するマスキングされた利用者属性情報を設定する。

【００６１】

ステップ８０７でアクセス要求処理部２１２は、利用者側処理装置１０１から送信されたアクセス内容の処理を実行する処理装置として設定したアクセス処理装置１０２に当該アクセス内容及び前記マスキングされた利用者属性情報を送り、当該アクセス内容の処理を前記設定したアクセス処理装置１０２に要求する。

【００６２】

ステップ８０８では、前記要求したアクセス内容の処理結果をアクセス処理装置１０２から受信しているかどうかを調べ、アクセス内容の処理結果を受信している場合にはステップ８０９へ進む。ステップ８０９では、前記受信した処理結果を当該アクセス内容の処理を依頼した利用者側処理装置１０１へ送信する。

【００６３】

図９は本実施形態のアクセス実行処理の処理手順を示すフローチャートである。図９に示す様にアクセス処理装置１０２のアクセス実行処理部４１１は、プロバイダ側処理装置１００から要求されたアクセス内容の処理をそのアクセス内容と共に送られた利用者属性に対応する範囲内で実行する処理を行う。

【００６４】

ステップ９０１でアクセス処理装置１０２のアクセス実行処理部４１１は、アクセス内容の処理要求をプロバイダ側処理装置１００から受信しているかどうか

を調べ、アクセス内容の処理要求を受信している場合にはステップ９０２へ進む。

【００６５】

ステップ９０２では、プロバイダ側処理装置１００から受信したマスキングされた利用者属性情報の内容とアクセス制御情報ＤＢ４０７中の情報提供ポリシーの内容とを比較してその利用者の利用者属性が情報提供ポリシーで示された条件を満たしているかどうかを調べる認証処理を行い、当該アクセス内容の処理を行う際のアクセス制御レベルを設定する。

【００６６】

ステップ９０３では、アクセス制御情報ＤＢ４０７中のアクセス制御情報の内容を参照し、前記設定したアクセス制御レベルの範囲内で当該アクセス内容の処理を実行する。ステップ９０４では、ステップ９０３でのアクセス内容の処理結果をプロバイダ側処理装置１００へ送信する。

【００６７】

以下に本実施形態のアクセス制御システムにおいて、利用者側処理装置１０１からインフルエンザに関する情報検索の処理をプロバイダ側処理装置１００に依頼し、当該情報検索を実行するアクセス処理装置１０２とそのアクセス処理装置１０２に開示する利用者属性の内容とを利用者属性開示ポリシーに従って決定する処理をプロバイダ側処理装置１００で行い、前記決定された開示内容の利用者属性に対応する範囲内で当該情報検索をアクセス処理装置１０２で実行する処理について説明する。

【００６８】

図７のステップ７０１で利用者側処理装置１０１のアクセス依頼処理部３１１は、ユーザＩＤ及びパスワードを送信してプロバイダ側処理装置１００にログインする。ステップ７０２では、利用者が要求するアクセス内容として、「インフルエンザにおいて可能な限り新しくかつ詳しい情報の検索」等の検索内容を入力し、ステップ７０３で検索内容情報としてメモリ３０２に格納する。ステップ７０４では、当該利用者の利用者属性の開示方針を示す利用者属性開示ポリシーとして図１０に示す様な情報を入力し、ステップ７０５で利用者属性開示ポリシー

情報としてメモリ３０２に格納する。

【００６９】

図１０は本実施形態の利用者属性開示ポリシーの一例を示す図である。図１０に示す様に本実施形態の利用者属性開示ポリシーでは、情報検索が行われるアクセス処理装置１０２の条件を示す情報として、サイト安全性・信頼性レベル「Ｂ」以上、プライバシー保護レベル「Ｂ」以上、大学、病院または医薬品企業のオフィシャルサイト、最終更新日時３ヶ月以内等が設定されており、そのアクセス処理装置１０２に対して開示する利用者属性情報の内容を示す情報として職業及び勤務先・役職が設定されている。

【００７０】

ステップ７０６では、前記格納した検索内容情報及び利用者属性開示ポリシー情報をネットワーク経由でプロバイダ側処理装置１００に送り、当該情報検索をプロバイダ側処理装置１００へ依頼する。

【００７１】

図８のステップ８０１でプロバイダ側処理装置１００の開示ポリシー処理部２１１は、情報検索依頼を利用者側処理装置１０１から受信してステップ８０２へ進み、ステップ８０２では、その情報検索の実行が可能なアクセス処理装置１０２からサイト情報として、図６に示した様な（株）△□製薬オフィシャルサイト、サイト安全性・信頼性レベル「Ａ」、プライバシー保護レベル「Ａ」、最終更新日：○○○○年○○月○○日等の情報を受信する。

【００７２】

ステップ８０３では、利用者側処理装置１０１から受信した利用者属性開示ポリシーのサイト安全性・信頼性レベル「Ｂ」以上、プライバシー保護レベル「Ｂ」以上、大学、病院または医薬品企業のオフィシャルサイト、最終更新日時３ヶ月以内等の情報と、アクセス処理装置１０２から受信したサイト情報の（株）△□製薬オフィシャルサイト、サイト安全性・信頼性レベル「Ａ」、プライバシー保護レベル「Ａ」、最終更新日：○○○○年○○月○○日等の情報とを比較して、そのアクセス処理装置１０２が利用者属性開示ポリシーで示された条件を満たしているかどうかを調べる認証処理を行い、ステップ８０４では、利用者属性開

示ポリシーの条件を満たしているアクセス処理装置１０２を当該情報検索の実行を行う処理装置として設定する。

【００７３】

ステップ８０５では、前記情報検索の実行が可能な全てのアクセス処理装置１０２からサイト情報を受信したかどうかを調べ、全てのアクセス処理装置１０２からサイト情報を受信し終えた場合にはステップ８０６へ進む。

【００７４】

ステップ８０６では、利用者側処理装置１０１から受信した利用者属性開示ポリシーに従って当該利用者のユーザＩＤに対応する職業「医師」及び勤務先・役職「○×病院院長」の情報を利用者属性ＤＢ２０７から読み出して、アクセス処理装置１０２へ開示するマスキングされた利用者属性情報を設定する。

【００７５】

ステップ８０７でアクセス要求処理部２１２は、前記情報検索を実行する処理装置として設定したアクセス処理装置１０２に当該検索内容及び前記マスキングされた利用者属性情報を送り、当該情報検索を前記設定したアクセス処理装置１０２に要求する。

【００７６】

ステップ９０１でアクセス処理装置１０２のアクセス実行処理部４１１は、情報検索要求をプロバイダ側処理装置１００から受信してステップ９０２へ進む。ステップ９０２では、プロバイダ側処理装置１００から受信したマスキングされた利用者属性情報の内容である職業「医師」及び勤務先・役職「○×病院院長」と、アクセス制御情報ＤＢ４０７中の情報提供ポリシーの内容とを比較してその利用者の利用者属性が情報提供ポリシーで示された条件を満たしているかどうかを調べる認証処理を行い、当該情報検索を行う際のアクセス制御レベルとしてレベル「Ａ」を設定する。

【００７７】

ステップ９０３では、アクセス制御情報ＤＢ４０７中のアクセス制御情報の内容を参照し、前記設定したレベル「Ａ」の範囲内で情報検索処理を行う。すなわちレベル「Ａ」では最新研究成果のアクセスが許されており、その最新研究成果

の情報が格納されたデータベースを検索する。ここで、レベル「Ａ」の範囲内ではそれ以下の情報にもアクセス可能であるものとし、レベル「Ｂ」の最新ウィルス種別及び対応ワクチンの情報が格納されたデータベース及びレベル「Ｃ」のインフルエンザについての情報が格納されたデータベースも検索するものとしても良い。ステップ９０４では、ステップ９０３での情報検索結果をプロバイダ側処理装置１００へ送信する。

【００７８】

ステップ８０８でプロバイダ側処理装置１００のアクセス要求処理部２１２は、前記の様に利用者属性に応じた最新研究成果を含む情報検索結果を受信し、ステップ８０９では当該情報検索を依頼した利用者側処理装置１０１へその情報検索結果を送信する。ステップ７０７で利用者側処理装置１０１のアクセス依頼処理部３１１は、当該利用者の利用者属性に応じた最新研究成果を含む情報検索結果を受信し、ステップ７０８でその情報検索結果を出力装置３０５へ表示する。

【００７９】

前記の様に本実施形態では、利用者の属性情報に応じてアクセス内容を処理するので、多くの利用者のユーザ管理に伴うアクセス処理装置１０２側での負担やリスクを増やすこと無く、利用者毎に木目細かなアクセス制御を行うことが可能である。

【００８０】

また本実施形態では、利用者属性の開示内容及び開示先を利用者属性開示ポリシーに従って制限しているので、利用者のプライバシーを保護することが可能である。更に本実施形態では、そのアクセス処理装置１０２が利用者属性開示ポリシーで示された条件を満たしているかどうかを調べる認証処理と、その利用者の利用者属性が情報提供ポリシーで示された条件を満たしているかどうかを調べる認証処理、すなわち利用者側のポリシーによる認証処理とアクセス処理装置１０２側のポリシーによる認証処理という双方向の認証処理を行っている為、より高度なアクセス制御を行うことが可能である。

【００８１】

また本実施形態では、各装置間で送受信される情報のインタフェースを統一し

、自動的に情報を要求・提供するエージェント技術に適用して、双方向認証、情報の要求／提供等の各種アクセス処理をエージェントによって実行することにより、木目細かな制御の完全な自動化を行うことが可能である。

【００８２】

以上説明した様に本実施形態のアクセス制御システムによれば、利用者から要求されたアクセス内容の実行を当該利用者の利用者属性に応じて制御するので、要求されたアクセス内容の実行側での利用者管理等の負担を増やすことなく利用者毎に木目細かなアクセス制御を行うことが可能である。

【００８３】

【発明の効果】

本発明によれば利用者から要求されたアクセス内容の実行を当該利用者の利用者属性に応じて制御するので、要求されたアクセス内容の実行側での利用者管理等の負担を増やすことなく利用者毎に木目細かなアクセス制御を行うことが可能である。

【図面の簡単な説明】

【図１】

本実施形態のアクセス制御システムの概略構成を示す図である。

【図２】

本実施形態のプロバイダ側処理装置１００の概略構成を示す図である。

【図３】

本実施形態の利用者側処理装置１０１の概略構成を示す図である。

【図４】

本実施形態のアクセス処理装置１０２の概略構成を示す図である。

【図５】

本実施形態の利用者属性ＤＢ２０７の一例を示す図である。

【図６】

本実施形態のアクセス制御情報ＤＢ４０７の一例を示す図である。

【図７】

本実施形態のアクセス依頼処理の処理手順を示すフローチャートである。

【図８】

本実施形態のアクセス要求処理の処理手順を示すフローチャートである。

【図９】

本実施形態のアクセス実行処理の処理手順を示すフローチャートである。

【図１０】

本実施形態の利用者属性開示ポリシーの一例を示す図である。

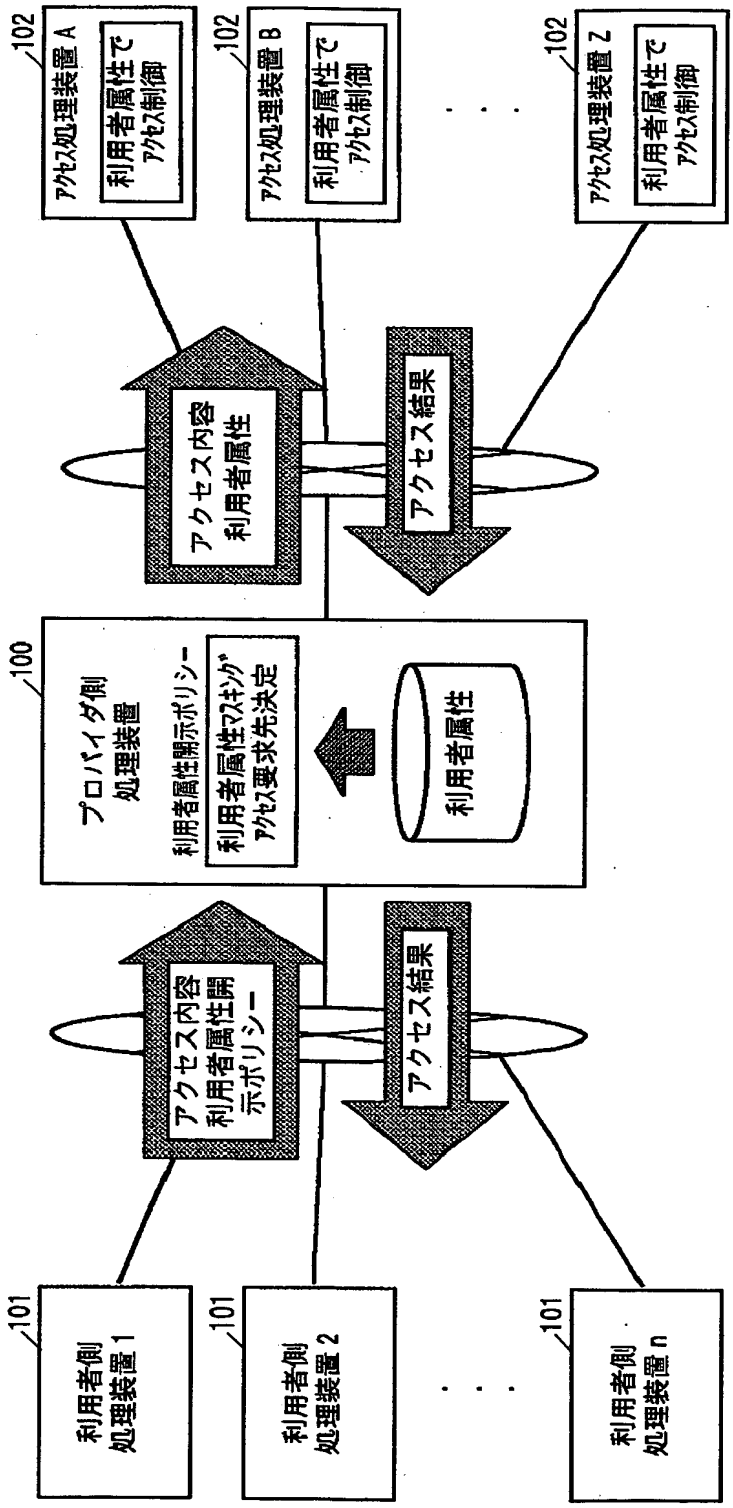
【符号の説明】

１００…プロバイダ側処理装置、１０１…利用者側処理装置、１０２…アクセス処理装置、２０１…ＣＰＵ、２０２…メモリ、２０３…磁気ディスク装置、２０４…入力装置、２０５…出力装置、２０６…ＣＤ－ＲＯＭ装置、２０７…利用者属性ＤＢ、２１０…利用者属性設定処理部、２１１…開示ポリシー処理部、２１２…アクセス要求処理部、３０１…ＣＰＵ、３０２…メモリ、３０３…磁気ディスク装置、３０４…入力装置、３０５…出力装置、３０６…ＣＤ－ＲＯＭ装置、３１０…利用者属性設定依頼処理部、３１１…アクセス依頼処理部、４０１…ＣＰＵ、４０２…メモリ、４０３…磁気ディスク装置、４０４…入力装置、４０５…出力装置、４０６…ＣＤ－ＲＯＭ装置、４０７…アクセス制御情報ＤＢ、４１０…アクセス制御情報設定処理部、４１１…アクセス実行処理部。

【書類名】　図面

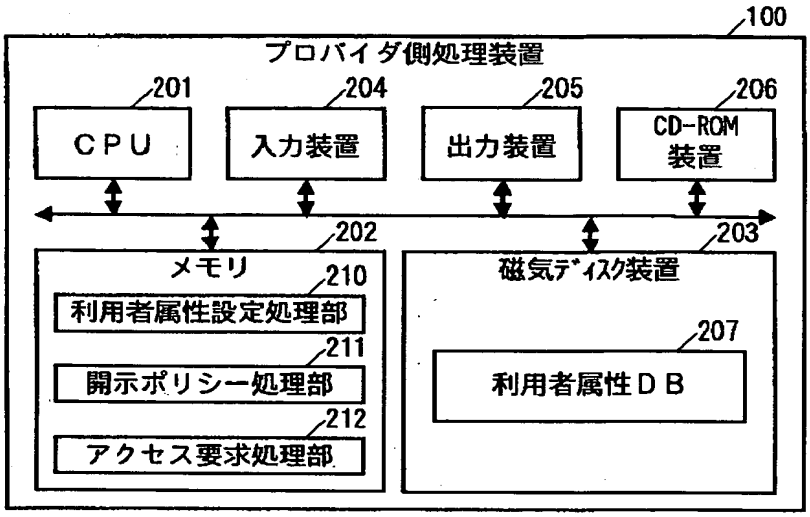
【図１】

図１


102
アクセス処理装置 A
利用者属性でアクセス制御
102
アクセス処理装置 B
利用者属性でアクセス制御
102
アクセス処理装置 Z
利用者属性でアクセス制御
アクセス内容
利用者属性
アクセス結果
100
プロバイダ側
処理装置
利用者属性開示ポリシー
利用者属性マスキングアクセス要求先決定
利用者属性
アクセス内容
利用者属性開示ポリシー
アクセス結果
101
利用者側
処理装置 1
101
利用者側
処理装置 2
101
利用者側
処理装置 n

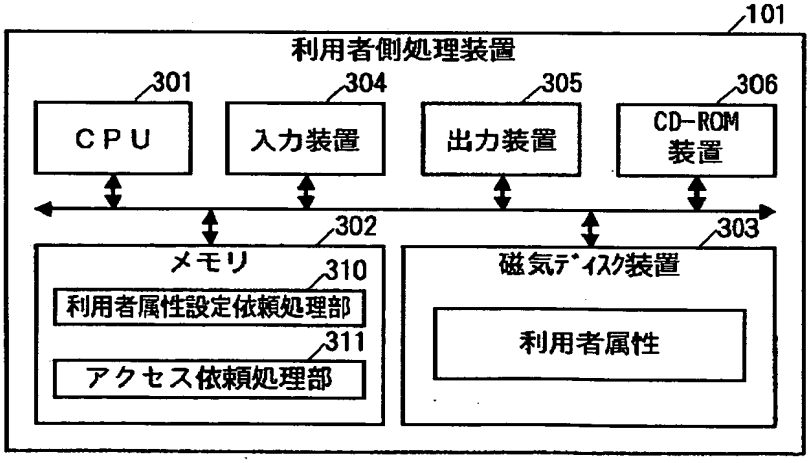
【図２】

図２


100
プロバイダ側処理装置
201
CPU
204
入力装置
205
出力装置
206
CD-ROM
装置
202
メモリ
210
利用者属性設定処理部
211
開示ポリシー処理部
212
アクセス要求処理部
203
磁気ディスク装置
207
利用者属性ＤＢ

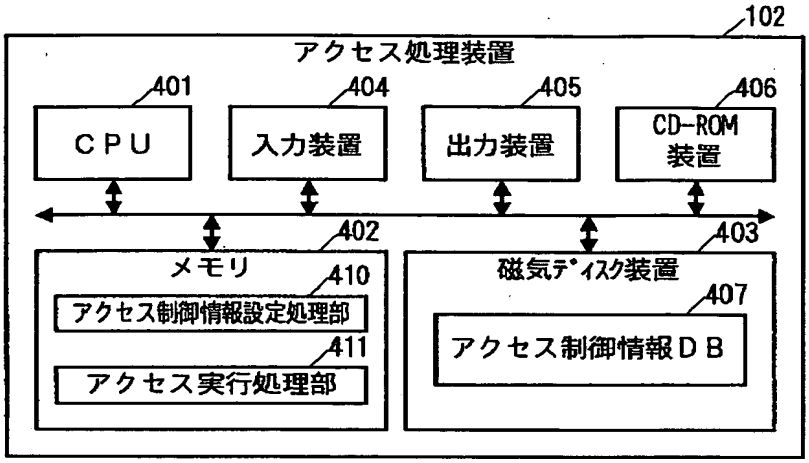
【図３】

図３


101
利用者側処理装置
301
CPU
304
入力装置
305
出力装置
306
CD-ROM
装置
302
メモリ
310
利用者属性設定依頼処理部
311
アクセス依頼処理部
303
磁気ディスク装置
利用者属性

【図４】

図４



【図５】

図５

207

ユーザＩＤ	氏名	性別	年齢	職業	勤務先・役職	：
0001	日立太郎	男	５５	医師	○×医院院長	：
0002	日立花子	女	３９	会社員	○□会社研究員	：
0003	鈴木三郎	男	２８	会社員	△□製薬	：
：	：	：	：	：	：	：

【図６】

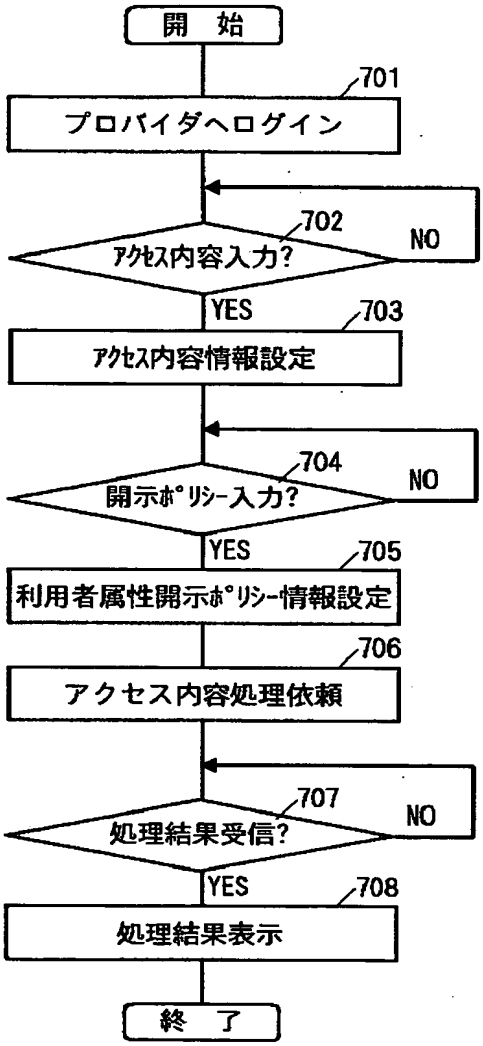
図６

アクセス制御情報のデータ構造　407

項番	項目名	内容
1	サイト公開者	（株）△□製薬
2	サイト情報	・　（株）△□製薬オフィシャルサイト ・　サイト安全性・信頼性レベル「Ａ」 ・　プライバシー保護レベル「Ａ」 ・　最終更新日：○○○○年○○月○○日
3	情報提供ポリシー	レベル「Ａ」：利用者属性の役職が「院長」 レベル「Ｂ」：利用者属性の職業が「医師」 レベル「Ｃ」：利用者属性の職業が「医師」以外 レベル「Ｄ」：利用者属性の提供無し
4	アクセス制御情報	レベル「Ａ」：最新研究成果 レベル「Ｂ」：最新ウィルス種別、対応ワクチン レベル「Ｃ」：インフルエンザについて レベル「Ｄ」：アクセス不可

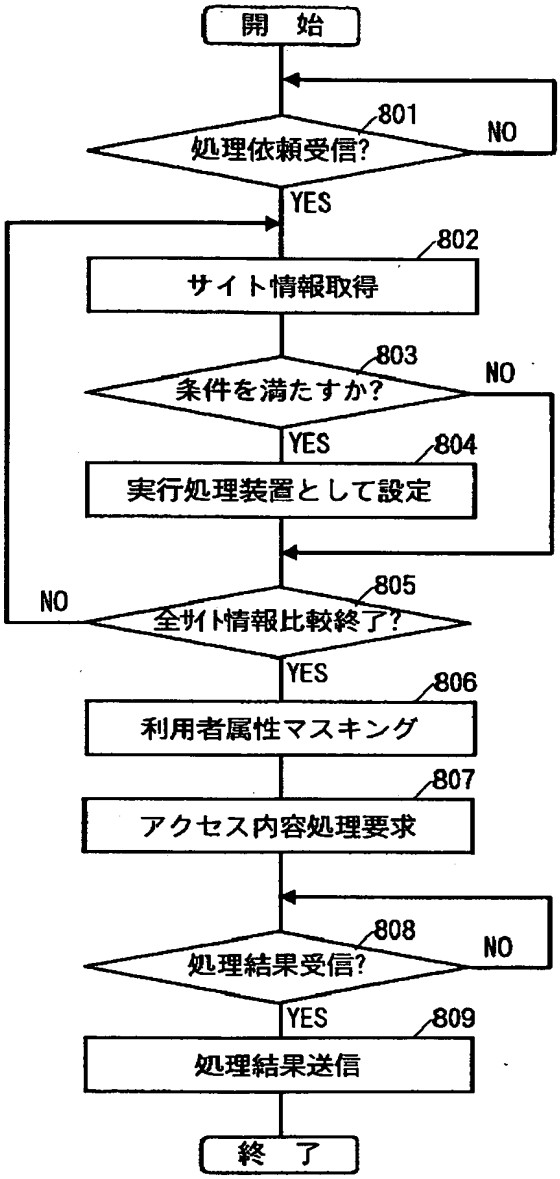
【図７】

図７


開　始
701
プロバイダへログイン
702
ｱｸｾｽ内容入力?
NO
YES
703
ｱｸｾｽ内容情報設定
704
開示ﾎﾟﾘｼｰ入力?
NO
YES
705
利用者属性開示ﾎﾟﾘｼｰ情報設定
706
アクセス内容処理依頼
707
処理結果受信?
NO
YES
708
処理結果表示
終　了

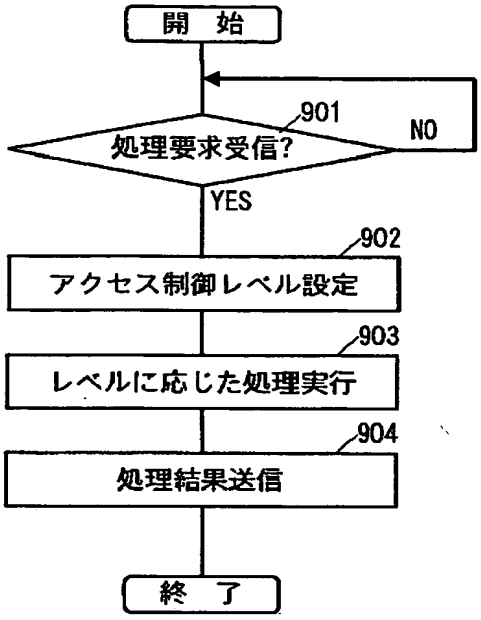
【図８】

図８


開　始
801
処理依頼受信?
NO
YES
802
サイト情報取得
803
条件を満たすか?
NO
YES
804
実行処理装置として設定
805
全サイト情報比較終了?
NO
YES
806
利用者属性マスキング
807
アクセス内容処理要求
808
処理結果受信?
NO
YES
809
処理結果送信
終　了

【図９】

図９



【図１０】

図１０

利用者属性 開示ポリシー	<u>アクセス処理装置の条件</u> 以下のすべてを満たすもの ・ サイト安全性・信頼性レベル「Ｂ」以上 ・ プライバシー保護レベル「Ｂ」以上 ・ 大学、病院または医薬品企業のオフィシャルサイトに限る ・ 最終更新日時３ヶ月以内
	<u>利用者属性開示内容</u> 職業 勤務先・役職

【書類名】　　要約書

【要約】

【課題】　要求されたアクセス内容の実行側での利用者管理等の負担を増やすことなく利用者毎に木目細かなアクセス制御を行うことが可能な技術を提供する。

【解決手段】　利用者から受付けたアクセス内容の実行を制御するアクセス制御方法において、利用者から要求されたアクセスの内容を示すアクセス内容を受付けるステップと、前記受付けたアクセス内容の実行を当該利用者の利用者属性と共に要求するステップと、前記要求されたアクセス内容の処理をそのアクセス内容と共に送られた利用者属性に対応する範囲内で実行するステップとを有するものである。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－２９７９３７
受付番号	５００００１２６０９２８
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年１０月　３日

＜認定情報・付加情報＞

【提出日】　平成12年 9月29日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所